in line 8, after "i.e.", insert --,--;

in line 10, cancel "protect the" and substitute --protect various aspects-- therefor, and cancel "with respect to the most varied aspects";

in line 12, cancel "A" and substitute --One-- therefor;

in line 13, after "the", insert --integrity of--;

in line 14, cancel "the so-called protection of the integrity of the data";

above line 16, insert

--**Description of the Related Art**--;

in line 17, cancel "the so-called" and substitute --a-- therefor;

in line 18, cancel ", for example" and substitute --such as-- therefor;

in line 19, cancel "[1]" and substitute --W. Stallings, Sicherheit in Netzwerk und Internet (Security in Network and Internet), Prentice Hall, ISBN 3-930436-29-9, pp. 203-223, 1995 (Stallings)-- therefor;

in line 20, cancel "[1]"and substitute --Stallings-- therefor;

in line 22, cancel "means" and substitute --way-- therefor;

in line 24, after "integrity", insert --of the data--;

in line 29, cancel "are matched" and substitute --match-- therefor;

in line 31, cancel "previously" and substitute --known-- therefor;

in line 32, cancel "necessitates that" and substitute --requires-- therefor, and cancel "must" and substitute --to-- therefor;

in line 35, cancel "since otherwise" and substitute --; if it is not,-- therefor;

in line 36, cancel "errored" and substitute --erroneous-- therefor; and

in line 39, after "segments", insert --,--.

On page 2, in line 2, cancel "or it is not" and substitute --; it may not be-- therefor;

in line 3, cancel "In the" and substitute --The-- therefor;

in line 4, cancel "from [1], it is therefore required for" and substitute --

described in Stallings requires-- therefor;

in line 6, cancel "that is to say";

in line 10, cancel "expenditure and substitute --overhead-- therefor;

in line 11, after "is", insert --even--;

in line 14, cancel "From [2], commutative" and substitute --Commutative-- therefor, and after "known", insert --from K. H. Kiyek and F. Schwarz, Mathmatik für Informatiker (Mathematics for Computer Scientists), Teubner Verlag, ISBN 3-519-03277-X, pp. 11-13, 1989 (Kiyek & Schwarz)--, and cancel "In [2]," and substitute --Kiyek & Schwarz include" therefor;

in line 15, cancel "is also specified. Illustratively, a commutative operation" and substitute --which-- therefor;

in line 18, cancel "each order" and substitute --any ordering-- therefor;

in line 19, cancel "operation" and substitute --operations-- therefor;

in line 21, cancel "EXOR" and substitute --exclusive OR (EXOR)-- therefor;

in line 23, cancel "From [3], a" and substitute --A-- therefor;

in line 26, after "known", insert --from German patent DE-A 2 048 365--;

above line 27, insert

--**SUMMARY OF THE INVENTION**--;

cancel lines 33-36, and substitute

--The object of the invention is achieved by a first method which forms a first commutative checksum for digital data grouped into a number of data segments by a computer, forming a first segment checksum for each data segment, forming a first commutative checksum by a commutative operation (⊕) on the first segment checksums, and cryptographically protecting the first commutative checksum using a cryptographic operation.

The object of the invention is also achieved with a second method which checks a predetermined cryptographic commutative checksum for digital data grouped into a number of data segments by a computer which has a predetermined

cryptographic checksum allocated to the digital data, and subjecting this cryptographic checksum to an inverse cryptographic operation to form a reconstructed first commutative checksum, forming a second segment checksum for each data segment, forming a second commutative checksum by a commutative operation on (⊕) the second segment checksums, and checking for a match between the second commutative checksum and the reconstructed first commutative checksum.

The object of the invention is also achieved with a third method which implements elements of both the first and second methods.

The object of the invention is also achieved with a first arrangement that forms a first commutative checksum for digital data grouped into a number of data segments which has an arithmetic and logic unit, a segment checksum that is formed for each data segment, a commutative operation that forms the first commutative checksum by operation on the segment checksums and a cryptographic operation that cryptographically protects the commutative checksum.

The object of the invention is also achieved with a second arrangement that checks a predetermined first commutative checksum allocated to digital data grouped into a number of data segments, that has an arithmetic and logic unit, an inverse cryptographic operation to form a first cryptographic checksum from a cryptographic commutative checksum formed by a cryptographic operation, a second segment checksum which is formed for each data segment, a commutative operation that operates on the second segment checksums which forms a second commutative checksum, and a comparator which checks for a match between the second commutative checksum and the first commutative checksum.

The object of the invention is also achieved with a third arrangement which implements elements of the first and second arrangements.--

On page 3, cancel lines 1 and 2.

in line 3, before "method", insert --first--, and cancel "according to Claim 1";

in line 9, before "method", insert --second--, and cancel "according to Claim 2";

in line 18, before "method", insert --third--, and cancel "according to Claim 3";

On page 4, in line 1, before "arrangement", insert --second--, and cancel "according to Claim 12", and cancel "exhibits" and substitute --has-- therefor;

in line 9, before "arrangement", insert --third--, and cancel "according to Claim 13", and cancel "exhibits" and substitute --has-- therefor;

On page 5, in line 2, cancel "the" and substitute --these-- therefor;

in line 3, cancel "the fact";

in line 5, after "received", insert --,--;

in line 7, before "checking", insert --data integrity--, and cancel "of the integrity of the data";

in line 9, cancel "Illustratively, the" and substitute --The-- therefor; and

in line 16, cancel "obtained from the dependent claims" and substitute --discussed below--.

On page 6, in line 1, cancel "so-called";

in line 17, cancel "," and substitute --in which-- therefor, and cancel "of which";

in line 25, cancel "Even if the" and substitute --The-- therefor;

in line 26, cancel "is"; and

in line 28, cancel ", this" and cancel "represent" and substitute --imply-- therefor.

On page 7, before line 1, insert

--**BRIEF DESCRIPTION OF THE DRAWINGS** -- ;

in line 1, cancel "The Figure shows" and substitute --The single Figure is a block diagram showing-- therefor, and cancel "," and substitute --in which-- therefore;

in line 2, after "segments", insert --are--;

above line 4, insert

--**DESCRIPTION OF THE PREFERRED EMBODIMENTS**--;

in line 7, after "data", insert --,--;

in line 8, cancel "it is of importance to ensure their integrity" and substitute --integrity must be maintained-- therefor;

in line 10, cancel "Both the" and substitute --The-- therefor;

in line 11, after "A2", insert --,--, and cancel "text" and substitute -- following text,-- therefor;

in line 12, cancel "which follows in each case" and substitute --each-- therefor;

in line 14, cancel "in the text which follows" and substitute --below-- therefor;

in line 19, cancel "[lacuna]" and substitute --formed-- therefor;

in line 20, cancel "checksum" and substitute --checksums-- therefor;

in line 22, cancel "[2]" and substitute --Kiyek & Schwarz-- therefor; and

in line 27, cancel "method" and substitute --operation-- therefor.

On page 8, in line 28, cancel "methods" and substitute --functions-- therefor;

On page 9, after "second", insert --segment--;

in line 4, after "further", insert --comparative--;

in line 15, cancel "and" and substitute --, possibly indicating-- therefor;

in line 16, cancel "is found and" and substitute --such a condition would-- therefor;

in line 20, cancel "so-called";

in line 24, after "first", insert --computer--;

in line 25, after "second", insert --computer--;

in line 30, cancel "In the text which follows" and substitute --The text below explains-- therefor; and

in line 31, cancel "will be explained".

On page 10, in line 12, before "independently", insert --either--, and cancel "However, the method for forming the checksum and the method for checking the checksum can also be" and substitute --or-- therefor;

in line 15, cancel "it is provided not to transmit digital data but" and substitute --the method also allows one-- therefor;

in line 16, cancel ", that is to say to store them" and substitute --by storing the digital data-- therefor;

in line 19, cancel "that is to say" and substitute --i.e.,-- therefor;

in line 25, cancel "Illustratively, the" and substitute --The-- therefor, and cancel "in that in the case of" and substitute --where-- therefor;

in line 26, cancel ",";

in line 27, cancel the first ",";

in line 32, cancel "take into consideration" and substitute --consider-- therefor; and

after line 33, insert --The above-described methods and arrangements are illustrative of the principles of the present invention. Numerous modifications and adaptions thereof will be readily apparent to those skilled in this art without departing from the spirit and scope of the present invention--.

a8

Cancel page 11.